PCSRF Conference Call Meeting Notes

Wednesday, May 26, 2004 1:30 PM – 3:00 PM EDT
Hosted by National Institute of Standards and Technology

Participants

Paul Blomgren, Mykotronx, Inc, a SafeNet Company
Derek Botfield, Starthis
Tony Capel, Comgate
Murray Donaldson, Decisive Analytics
Terry Fletcher, Decisive Analytics
Tom Good, DuPont
Mike Hammon, Illinois Power
Charles Hoover, Rockwell
Ian Kinakde, Indormation Design, Inc.
Linda Lassen, Indormation Design, Inc.
Ron Melton, Decisive Analytics
Bill Miller, MaCT
David Naylor, Starthis
Robert O'Bien, Indormation Design, Inc.
Dick Oyen, ABB
Dale Peterson, DigitalBond
Tom Phinney, Honeywell
Ernest Rakaczky, Invensys
Ted Ripp, BP
Marty Robbins, Georgia Pacific
David Saunders, Westin
Ron Sielinski, Microsoft
Walter Sikora, Verano
Joseph D. Steller, American Lifelines Alliance, National Institute of Building Sciences
Keith Stouffer, NIST

Purpose

The main objective for the meeting was to review/discuss Version 1.0 of the System Protection Profile for Industrial Control Systems (SPP-ICS) document.

Agenda

- System Protection Profile for Industrial Control Systems (SPP-ICS) Version 1.0 review
- SPP-ICS comments/discussion
- Direction and next steps
- News and status updates

Opening Remarks

Keith Stouffer (NIST) started off the meeting stating that there are now approximately 500 registered members in PCSRF, many who are relatively new to the group. Therefore, this meeting took a little step backward to provide some background information on the effort so that we get everyone on the same page. That will allow the group to gather the energy and the momentum required to make our next push forward in this effort

The main topic for this conference call is to review the 1.0 Version of the System Protection Profile for Industrial Control Systems (SPP-ICS). The SPP-ICS document is designed to present a cohesive, cross-industry, baseline set of security requirements for new industrial control systems. These security capabilities would be specified in procurement RFPs for new industrial control systems. The SPP-ICS considers an entire system and addresses requirements for the entire system lifecycle. The SPP-ICS also acts as a starting point for more specific system protection profiles (SCADA, DCS, etc.), for a specific industry (water, oil/gas, etc.), and for component protection profiles (industrial controller authentication, encryption modules, sensor authentication, etc).

The document is designed to be an industry voice to the industrial control system vendors and system integrators, the security capabilities that are desired in new products and systems. This is not a NIST or a DA standard that is going to be forced upon you and expected to comply with. It is your document to specify the security capabilities that are desired in new products and systems and we need your input to make sure that it accurately reflects this.

SPP-ICS Review

The main objective for the meeting was to review/discuss Version 1.0 of the System Protection Profile for Industrial Control Systems (SPP-ICS) document. Ron Melton (Decisive Analytics) gave a presentation on the SPP-ICS that:

- Provided some background on the SPP-ICS
- Defined what is a System Protection Profile
- Described the structure of the SPP-ICS
- Described what has changed from V0.91 to V1.0
- Described how to use the SPP-ICS

The full presentation along with audio is available on the PCSRF website at:
http://www.isd.mel.nist.gov/projects/processcontrol/members/minutes/26-May-2004/SPP-ICS-26-May-04.ppt

SPP-ICS comments/discussion

Keith Stouffer (NIST) asked if the list of extensions to the Common Criteria to address system level issues that were developed from the PCSRF and ISO/IEC 19791 efforts is available. Murray Donaldson (Decisive Analytics) said that a full list of the newly developed extensions exists and he will look into the possibility of making the list available to the PCSRF group.

Dale Peterson (Digitalbond) added that this list of extensions would be valuable to review.

Bill Miller (MaCT) asked if whether the ISO/IEC 17799 framework was used for the SPP-ICS. Murray Donaldson responded that aspects of ISO/IEC 17799 and NIST SP800-53 were used in the development of the SPP-ICS.

Dick Oyen (ABB) added that ISA TR3 was reviewing the definition on terms in ISO/IEC 17799 to make sure that TR3 does not create conflicting definitions of terms.

There was some discussion on the certification aspect of the PCSRF effort. Keith Stouffer posed the question “Do people feel that certification of products/systems is required/positive thing or as long as the security capabilities are present in the products certification may not be necessary?”

Ron Sielinski (Microsoft) said that the end user drives whether certification is something of value and is worth paying the extra cost for.

Tom Good (DuPont) added that certification may not be required as long as the vendor backs their statements of meeting requirements through structured rigorous testing, etc.

Ernest Rakaczky (Invensys) added that certification could create a false sense of security because things change from the initial installation. Murray Donaldson, Ron Melton and Keith Stouffer added that this issue is main reason for addressing security throughout the life of the system in a structured approach. Security is a lifecycle effort and the system can't just be installed and left because the security environment does change.

Bill Miller (MaCT) added that some aspects of certification, such as system certification, are good.

Direction and next steps

Several next steps were discussed during the call. One step discussed was to develop a plain English guidance document on how to use the SPP-ICS to specify security requirements for products and systems in your procurement documents. This is something that is of interest to the group and will be pursued when funding is available.

The group also discussed reviewing additional protection profiles such as the Control Center Protection Profile that Dale Peterson presented at the last PCSRF meeting and other SPP-ICS derived protection profiles such as a SCADA specific protection profile. The group agreed that this was valuable.

News and status updates

Joe Steller (ALA, NIBS) mentioned that ASTM E54.06 is a new subcommittee addressing Security Controls and may be a good group to contact with information on the SPP-ICS. Keith Stouffer responded that he will make contact with them this week.

Ron Melton asked that if people are interested in the training discussed during the presentation that they send an email to **CCTraining@dac.us**

Next Meeting

The next meeting will be a conference call during the month of August 2004. Additional information, including a request for available dates will be sent out shortly to the group.